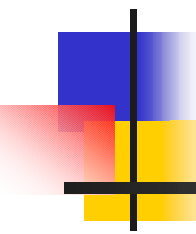


Securing Mobile Networks

An Enabling Technology for National and International Security and Beyond

Goals for November 6th

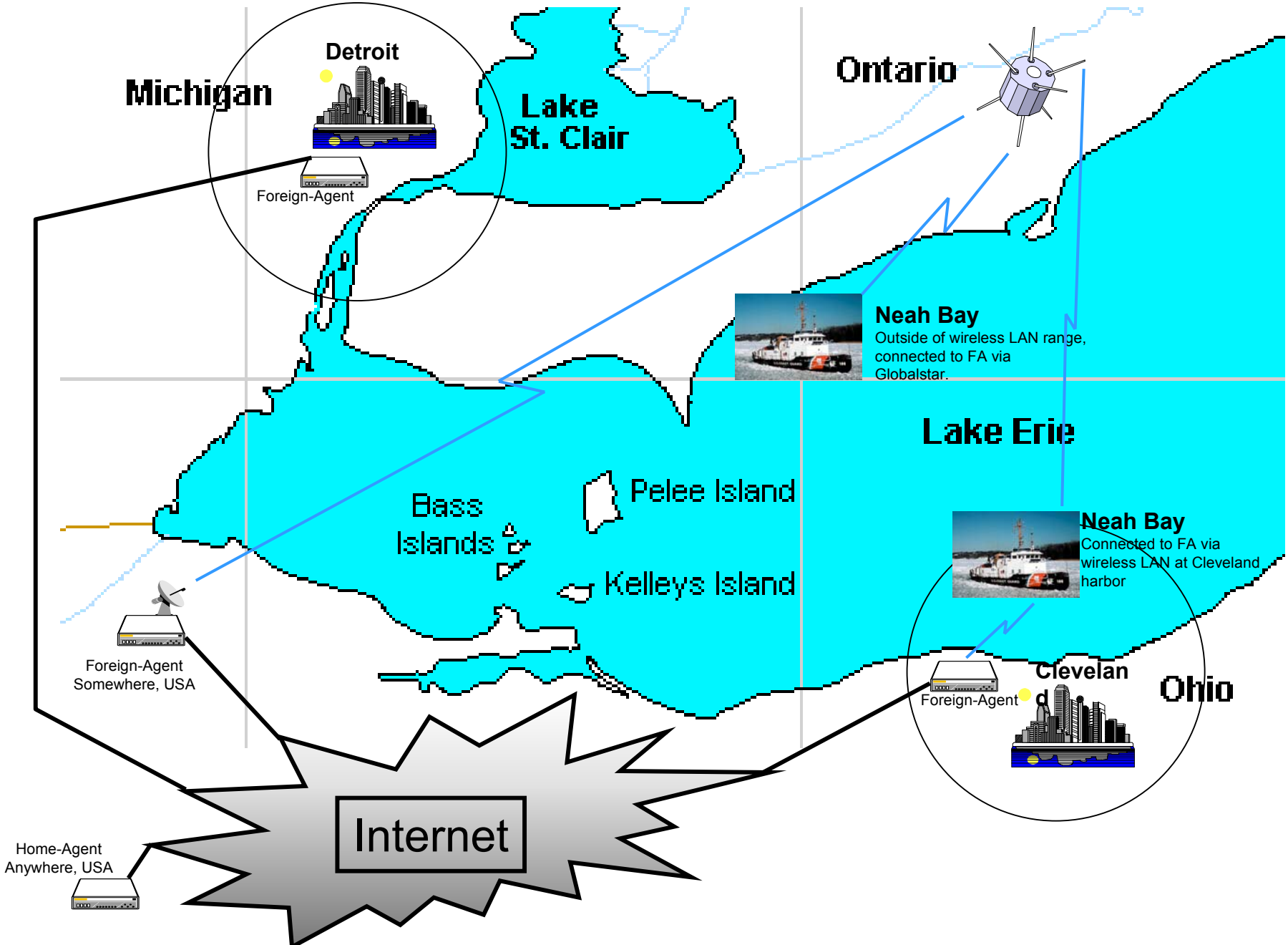
- Highlight Mobile Networking Technology
  - Emphasizing National and International Security today due to time limitations.
- Discuss security policy
  - Enabling shared infrastructure (when reasonable)
- Next Steps (Afternoon Session)
- Other Items (Afternoon Session)

Today's Audience

- Big Picture People
- Policy Makers
- Media
- Code Writers
- Implementers

Please, don't be afraid to ask questions.

Neah Bay / Mobile Router Project

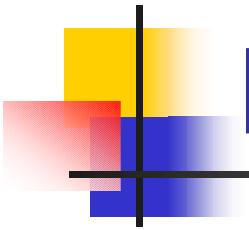


Why NASA/USCG/Industry

- Real world deployment issues can only be addressed in an operational network.
- USCG has immediate needs, therefore willingness to work the problem.
- USCG has military network requirements.
- USCG is large enough network to force us to investigate full scale deployment issues
- USCG is small enough to work with.
- NASA has same network issues regarding mobility, security, network management and scalability.

Mobile-Router Advantages

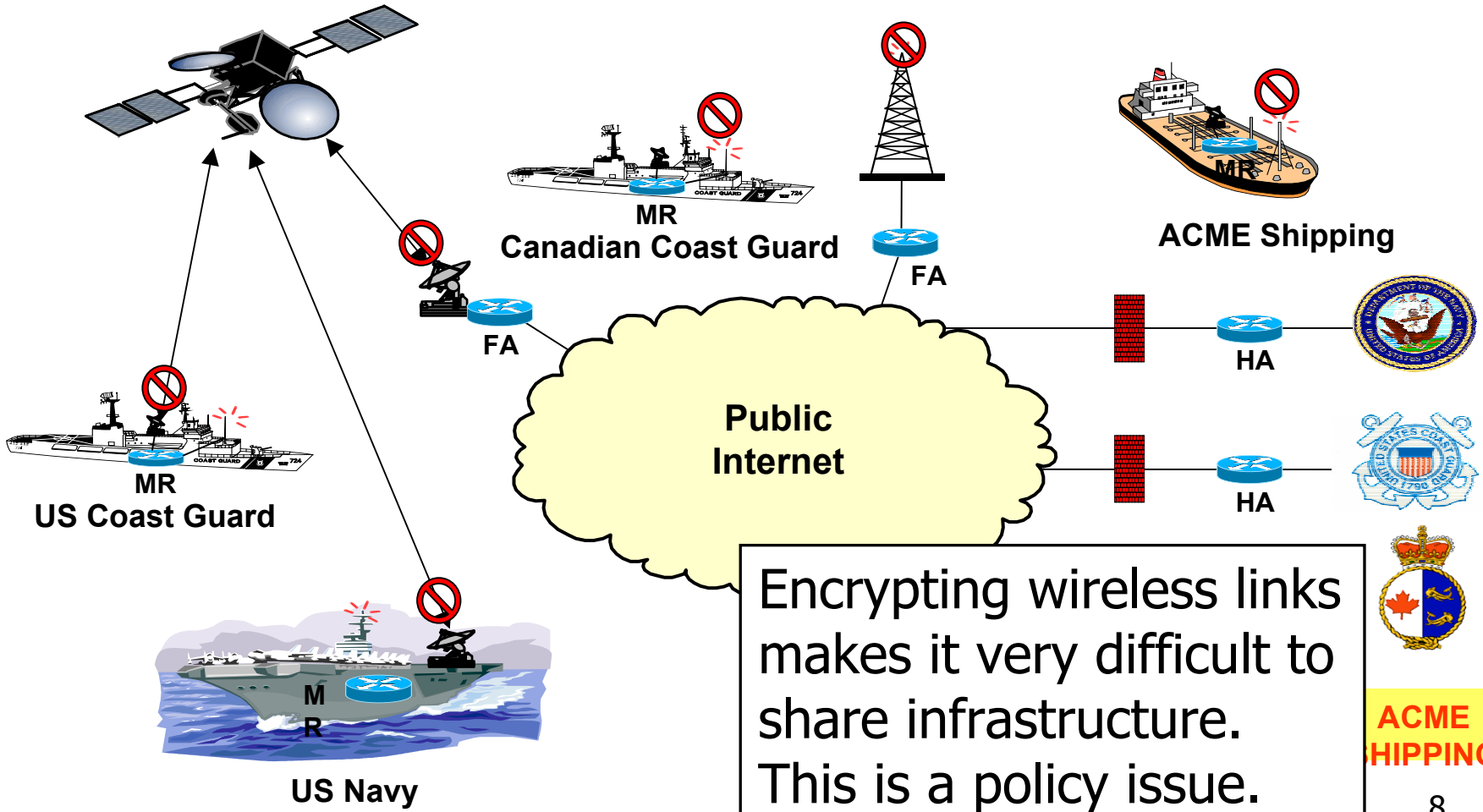
- Share wireless and network resources with other organizations
  - $$$ savings
- Set and forget
  - No onsite expertise required
  - However, you still have to engineer the network
- Continuous Connectivity
  - (May or may not be important to your organization)
- Robust
  - Secondary Home Agent (Reparenting of HA)



Mobile Network Design Goals

- Secure
- Scalable
- Manageable
- Ability to sharing network infrastructure
- Robust

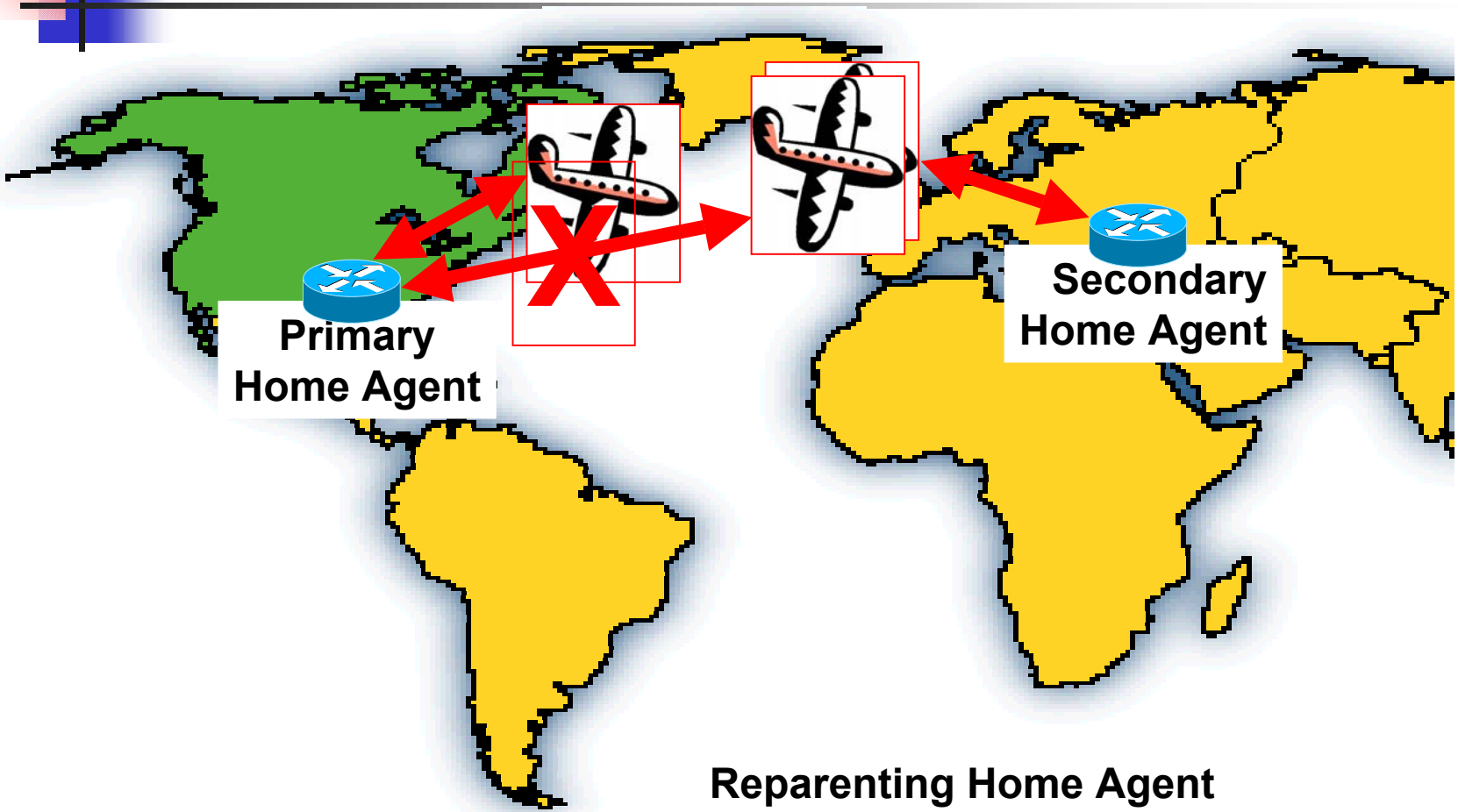
Shared Network Infrastructure



Encrypting wireless links makes it very difficult to share infrastructure. This is a policy issue.

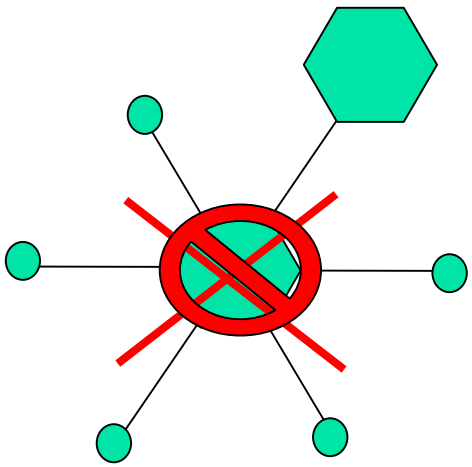
ACME SHIPPING

Secondary Home Agent (reparenting the HA)



Reparenting Home Agent
Helps resolve triangular routing
Problem over long distances

Emergency Backup (Hub / Spoke Network)

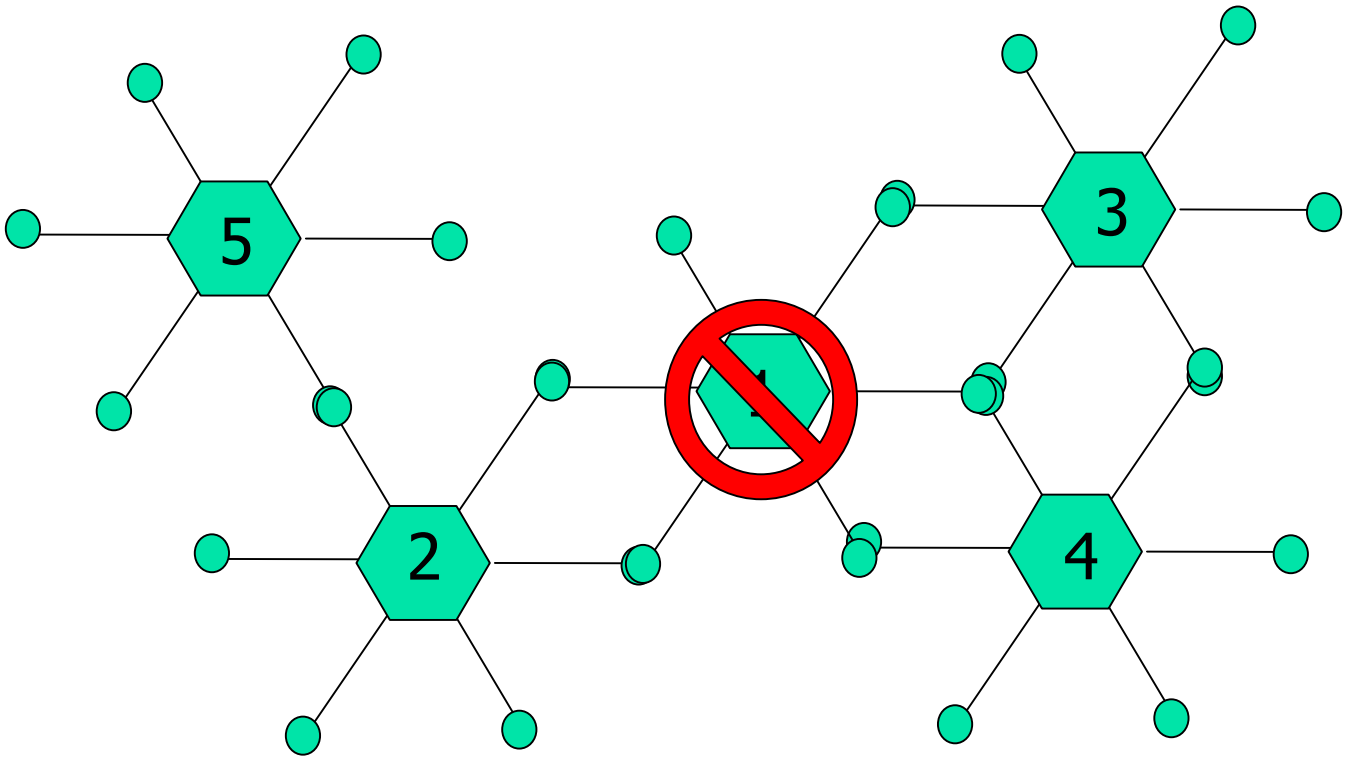


If primary control site becomes physically inaccessible but can be electronically connected, a secondary site can be established.

If primary control site is physically incapacitated, there is no backup capability.

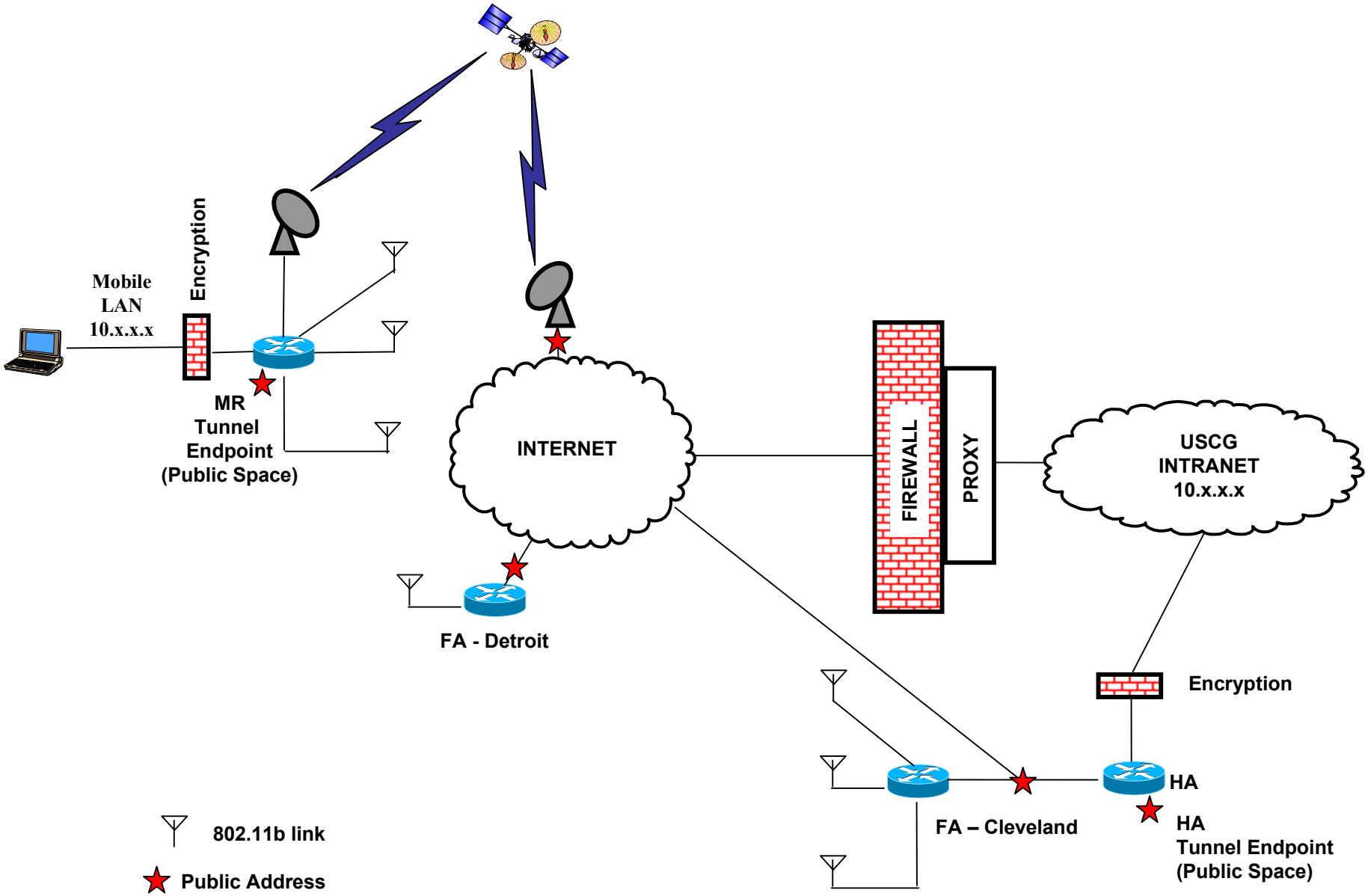
Secondary Home Agent (Fully Meshed Network)

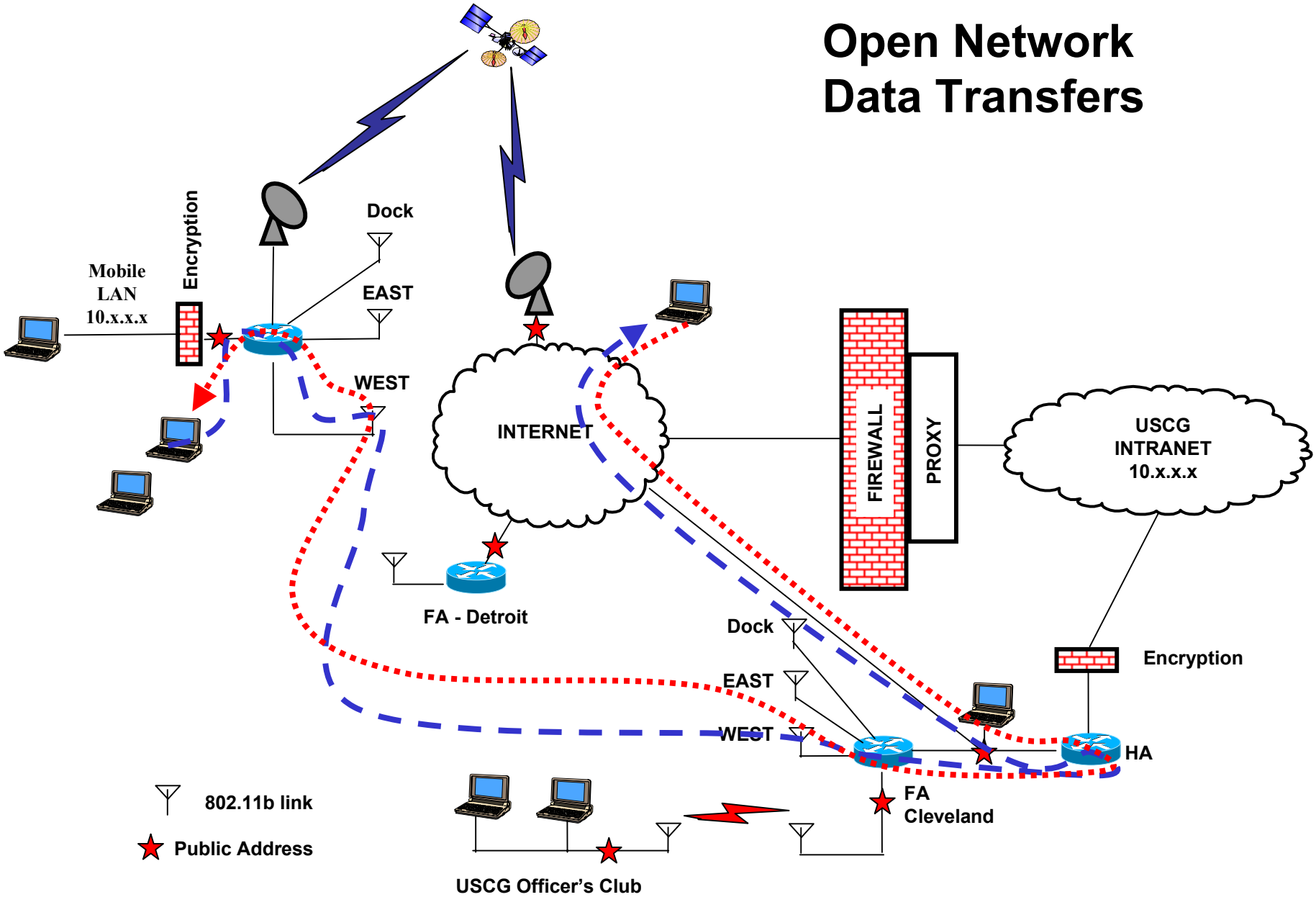
If primary control site is physically incapacitated, a second or third or forth site take over automatically.

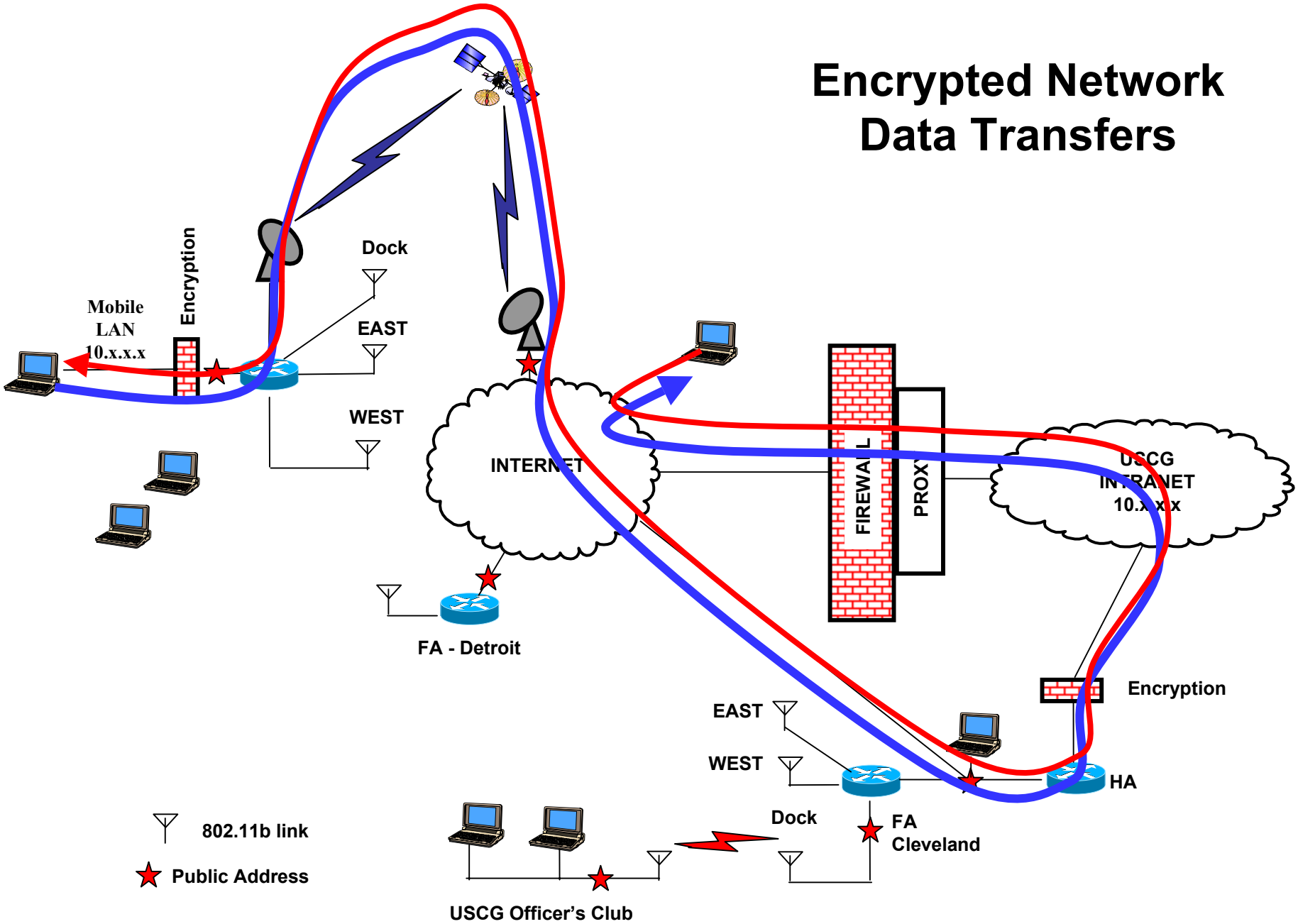


We Are Running with Reverse Tunneling

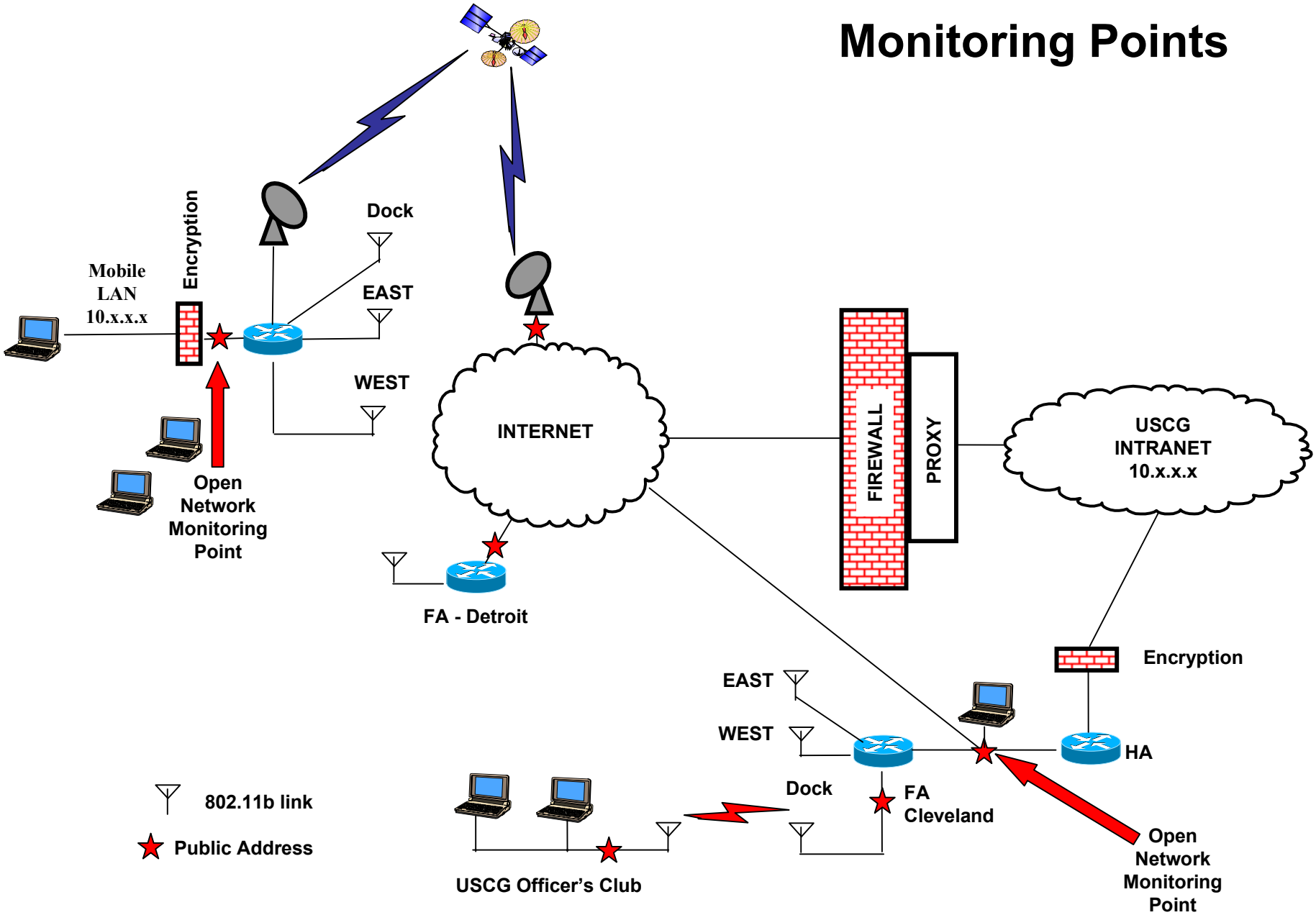
- Pros
  - Ensures topologically correct addresses on foreign networks
  - Required as requests from MR LAN hosts must pass through Proxy inside main firewall
  - Greatly simplifies setup and management of security associations in encryptors
  - Greatly simplifies multicast – HA makes for an excellent rendezvous point.
- Cons
  - Uses additional bandwidth
  - Destroys route optimization

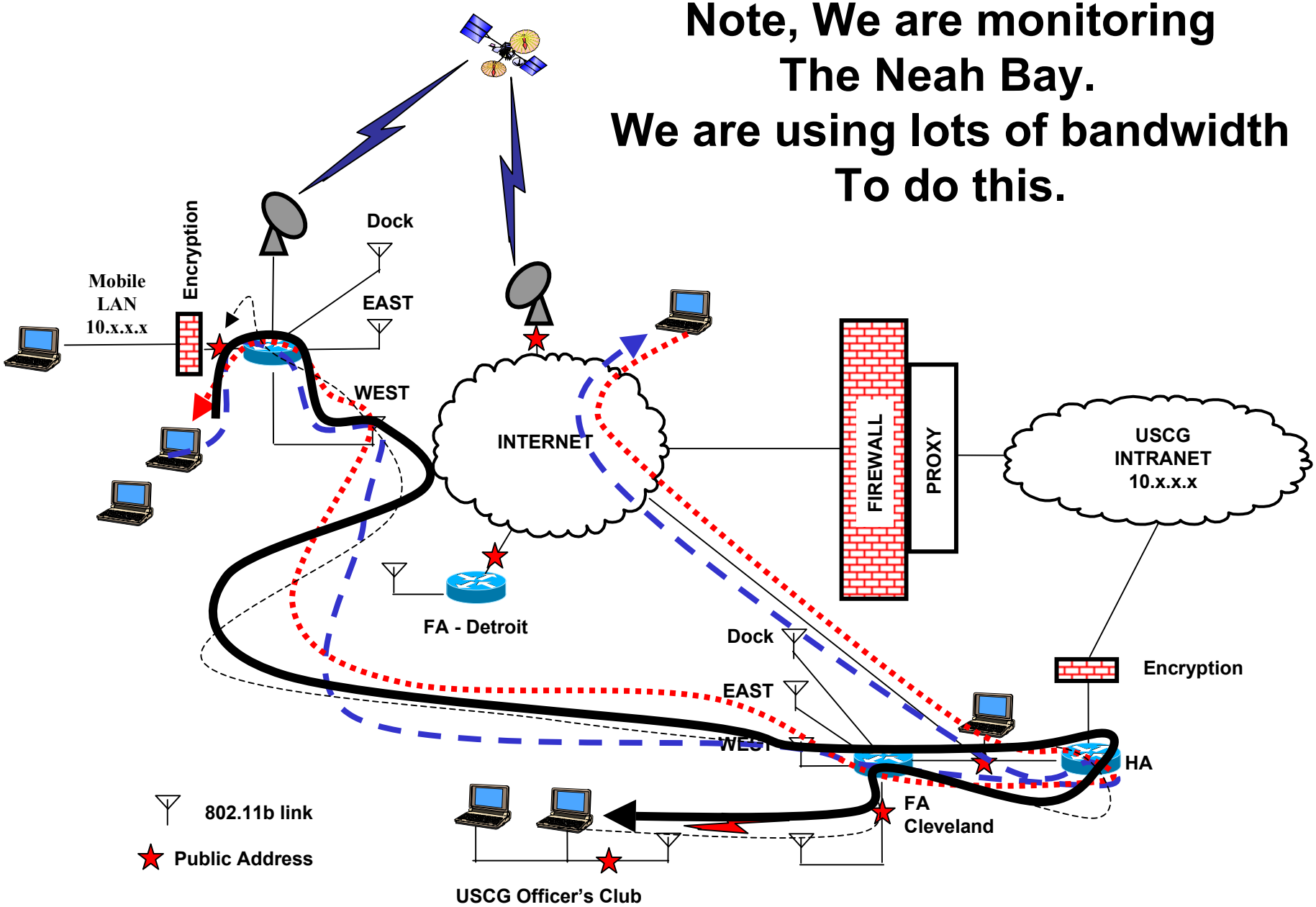

Mobile
LAN
10.x.x.x
Encryption
MR
Tunnel
Endpoint
(Public Space)
INTERNET
FIREWALL
PROXY
USCG
INTRANET
10.x.x.x
FA - Detroit
Encryption
HA
HA
Tunnel Endpoint
(Public Space)
FA – Cleveland
802.11b link
Public Address

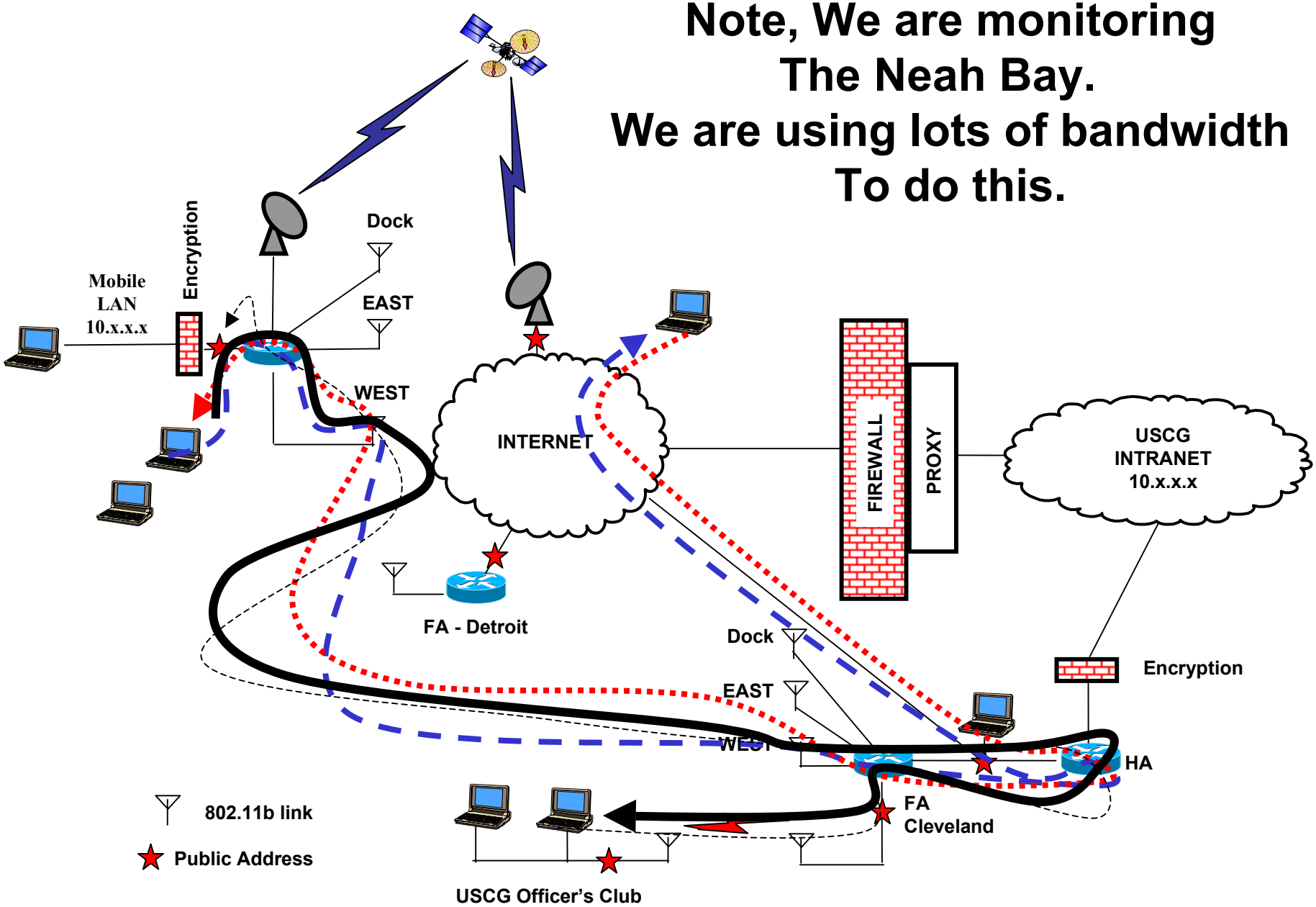

Open Network
Data Transfers
Mobile
LAN
10.x.x.x
Encryption
Dock
EAST
WEST
INTERNET
FIREWALL
PROXY
USCG
INTRANET
10.x.x.x
FA - Detroit
Dock
EAST
WEST
Encryption
HA
FA
Cleveland
802.11b link
Public Address
USCG Officer's Club


Encrypted Network
Data Transfers
Mobile
LAN
10.x.x.x
Encryption
Dock
EAST
WEST
INTERNET
FIREWALL
PROXY
USCG
INTRANET
10.x.x.x
FA - Detroit
Encryption
EAST
WEST
HA
Dock
FA
Cleveland
802.11b link
Public Address
USCG Officer's Club

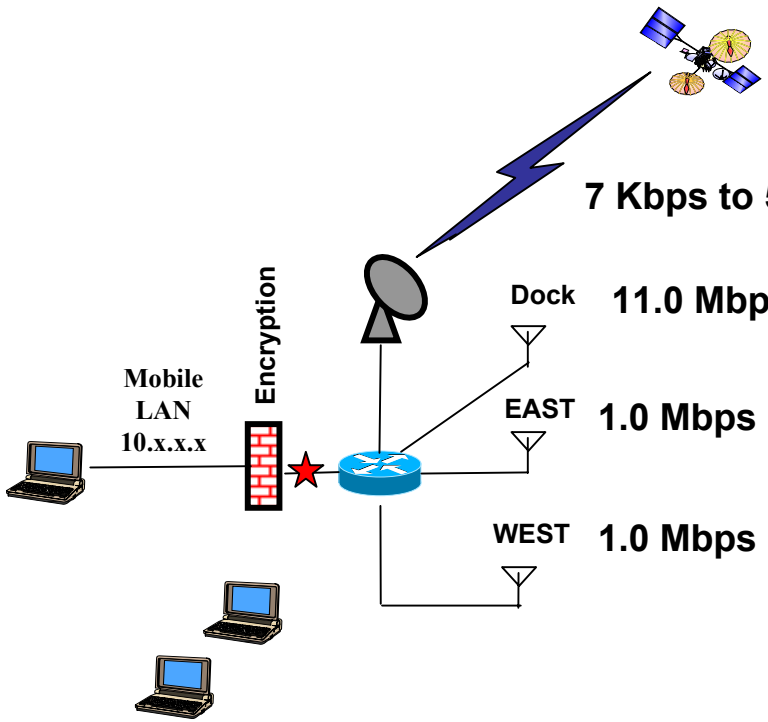
Monitoring Points




Note, We are monitoring
The Neah Bay.
We are using lots of bandwidth
To do this.
Mobile
LAN
10.x.x.x
Encryption
Dock
EAST
WEST
INTERNET
FIREWALL
PROXY
USCG
INTRANET
10.x.x.x
FA - Detroit
Dock
EAST
WEST
Encryption
HA
FA
Cleveland
802.11b link
Public Address
USCG Officer's Club


Note, We are monitoring
The Neah Bay.
We are using lots of bandwidth
To do this.
Mobile
LAN
10.x.x.x
Encryption
Dock
EAST
WEST
INTERNET
FIREWALL
PROXY
USCG
INTRANET
10.x.x.x
FA - Detroit
Dock
EAST
WEST
Encryption
HA
FA
Cleveland
802.11b link
Public Address
USCG Officer's Club

RF Bandwidth

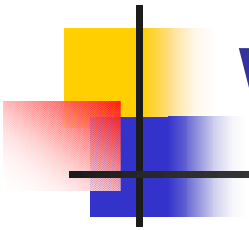


7 Kbps to 56 Kbps in 7 Kbps chunks (1 to 2.5 seconds delay)

11.0 Mbps (auto-negotiated and shared with Officer's Club)

1.0 Mbps (manually set)

1.0 Mbps (manually set)



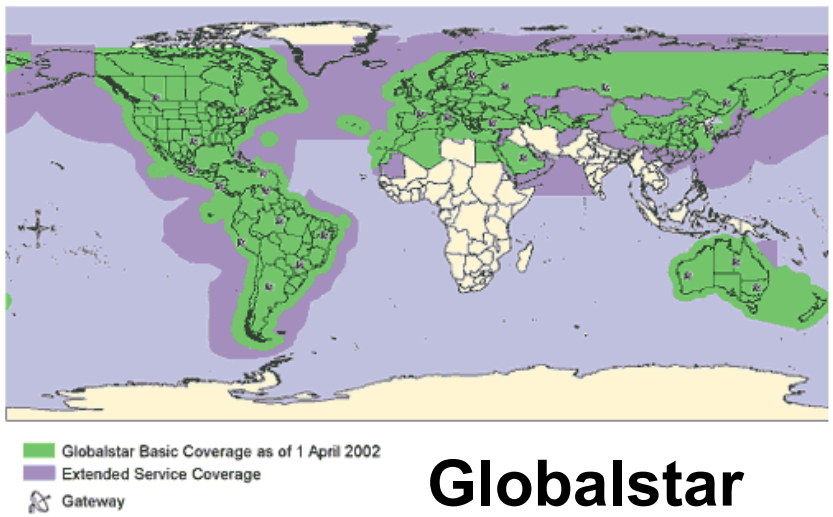
Wireless Only?

- Wireless can be jammed
  - Particularly unlicensed spectrum such as 802.11
  - Satellites is a bit harder
  - Solution is to find interferer and make them stop.
- You still want land line connections
  - Mobile Routing can be used over land lines.

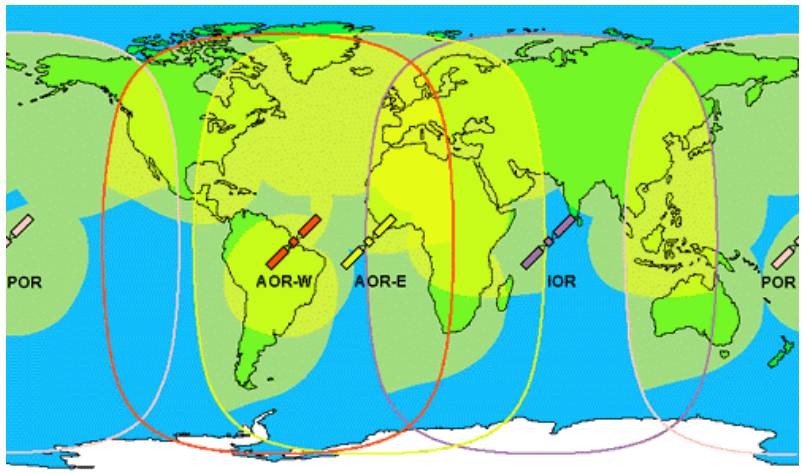
Globalstar/Sea Tel MCM-8

- Initial market addresses maritime and pleasure boaters.
- Client / Server architecture
  - Current implementation requires call to be initiated by client (ship).
  - Multiplexes eight channels to obtain 56 kbps total data throughput.
  - Full bandwidth-on-demand.
- Requires use of Collocated Care-of-Address

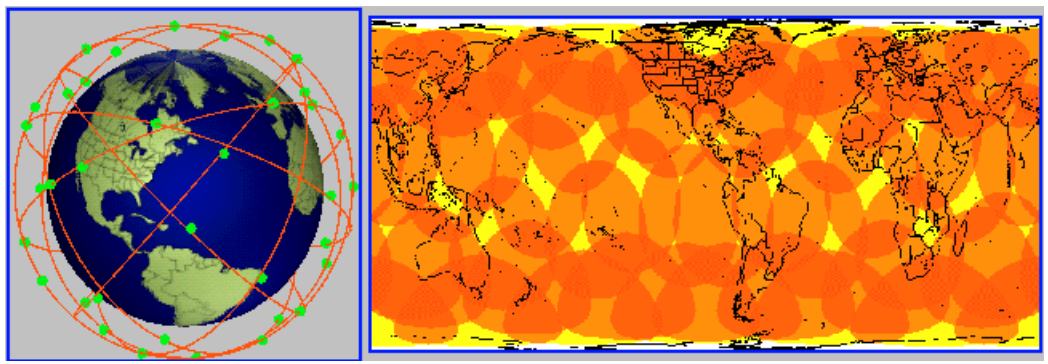
Satellite Coverage



Globalstar



INMARSAT



From SaVi

Layer 2 Technology

Globalstar
MCM-8

L3-Comm
15 dBic
Tracking Antenna

8 dBi
Dipole

Hypergain
802.11b
Flat Panel

Sea Tel Tracking
Antenna

Backbone Network Topology

Detail Network Diagram

(Intentionally Blank)

Neah Bay Network Topology

Detail Network Diagram

(Intentionally Blank)

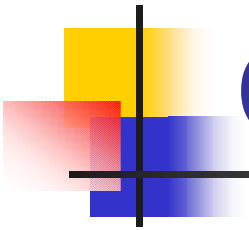
USCG Officer's Club Network Topology

Detail Network Diagram

(Intentionally Blank)

Securing Mobile and Wireless Networks

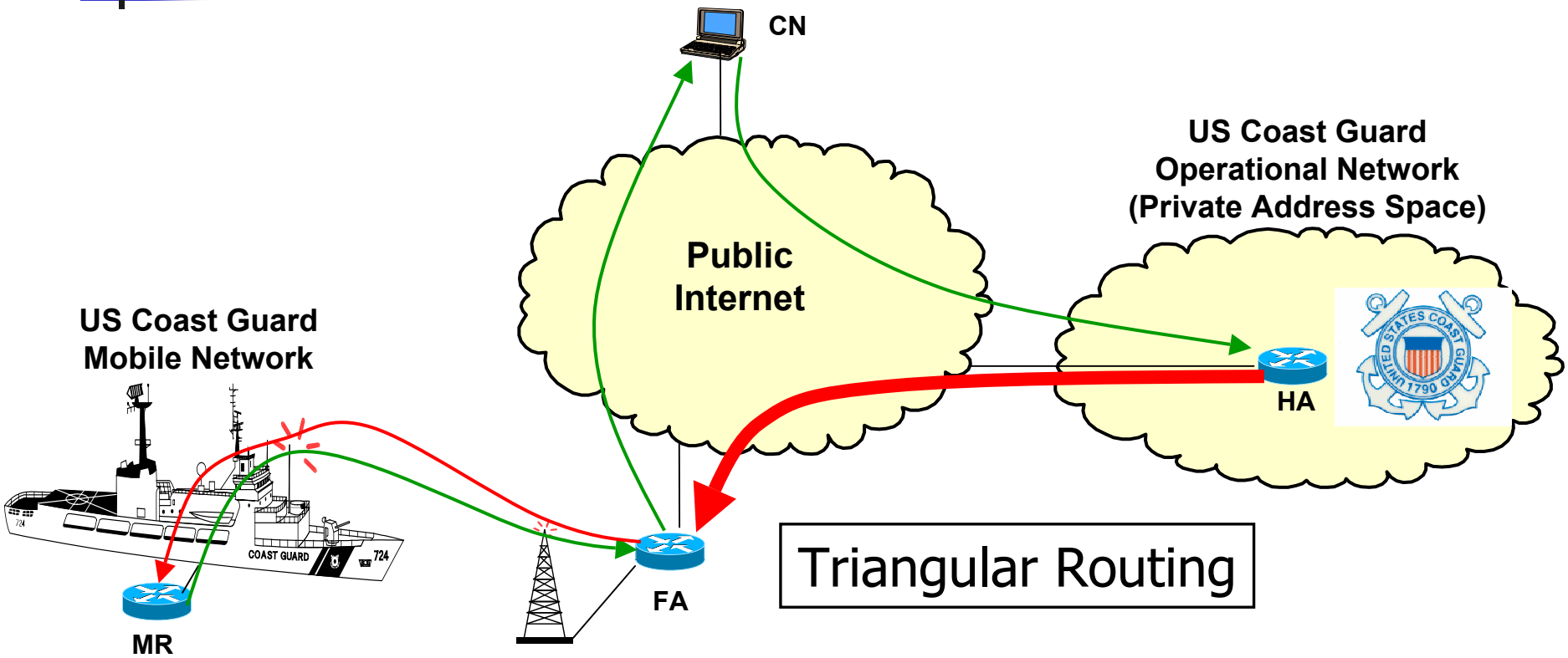
Some ways may be “better” than others!



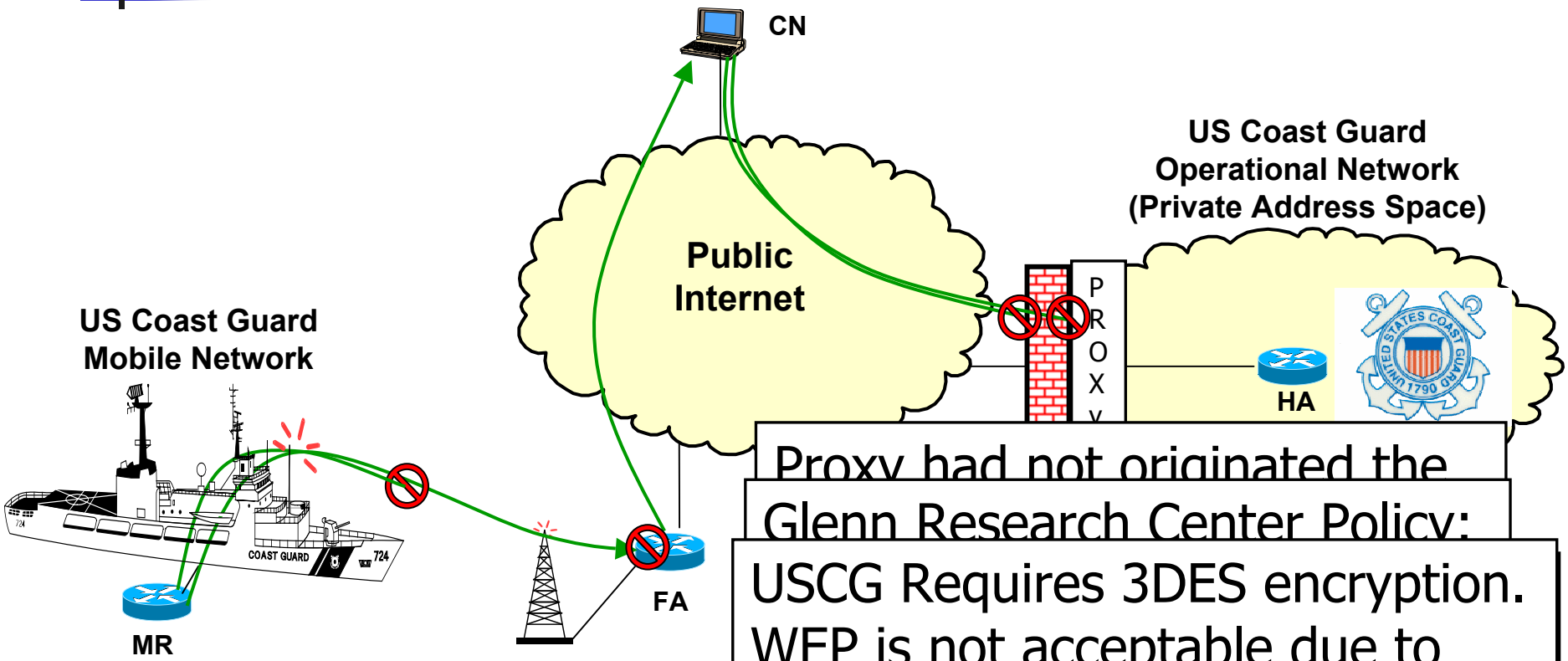
Constraints / Tools

- Policy
- Architecture
- Protocols

IPv4 Utopian Operation



IPv4 "Real World" Operation



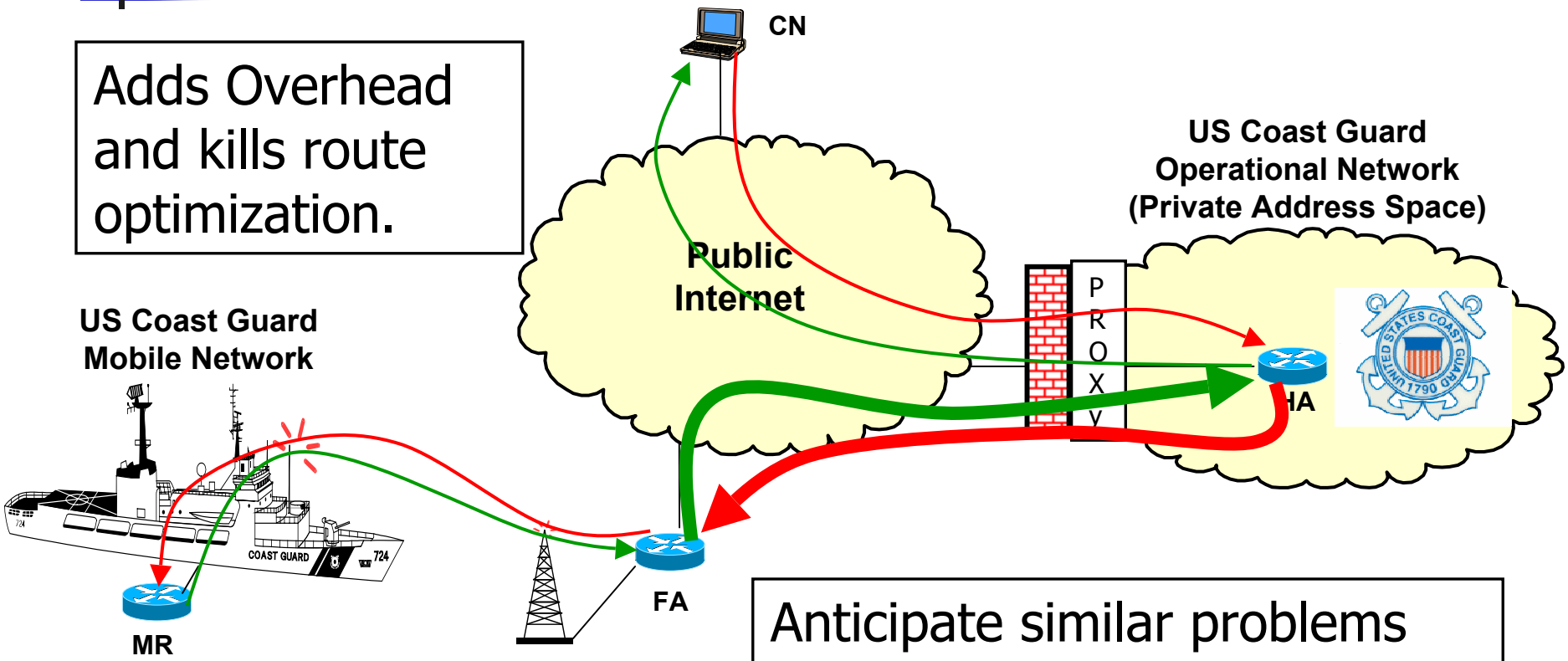
Proxy had not originated the Glenn Research Center Policy:

USCG Requires 3DES encryption. WEP is not acceptable due to known deficiencies.

Corrects this problem.

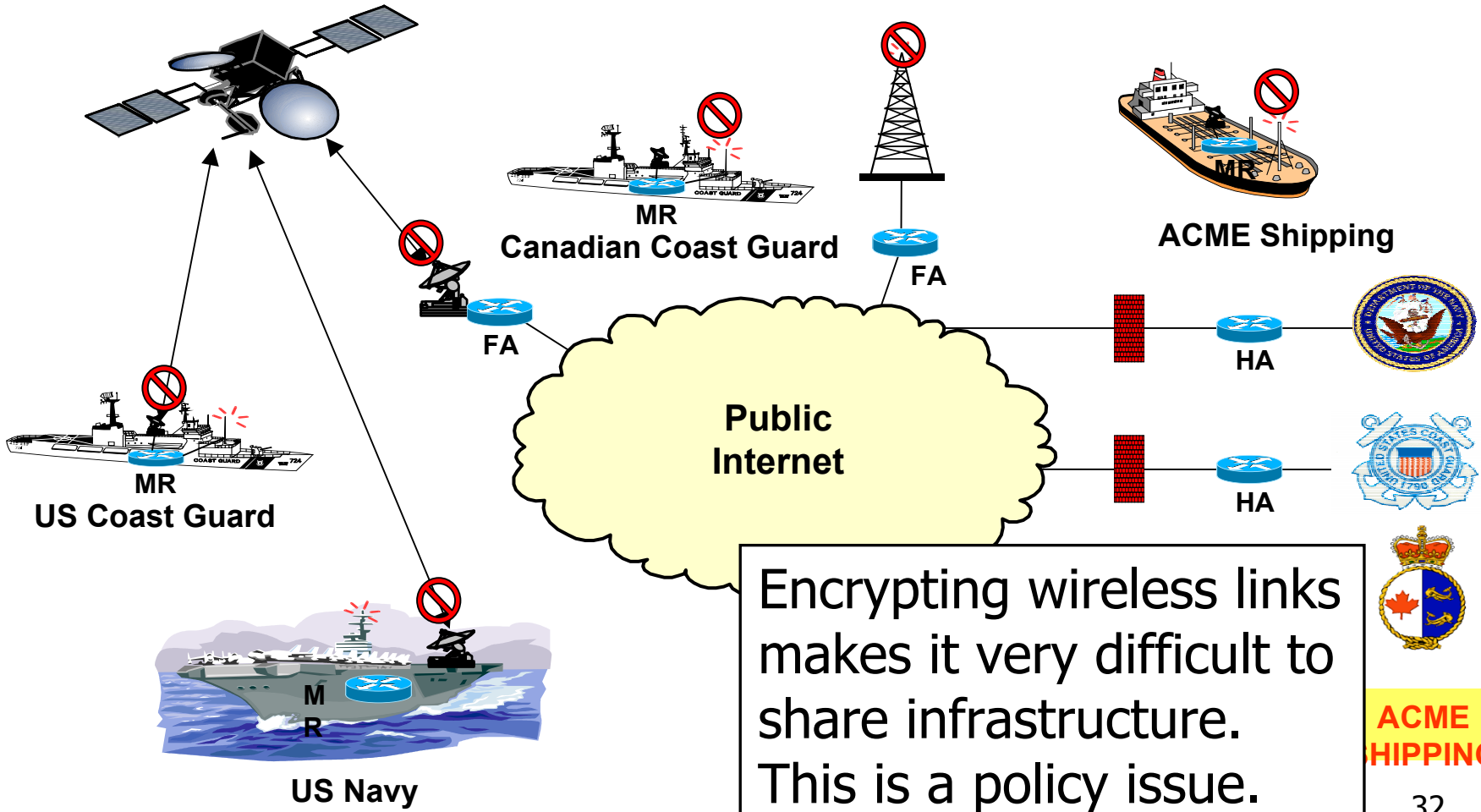
Current Solution – Reverse Tunneling

Adds Overhead and kills route optimization.



Anticipate similar problems for IPv6.

Shared Network Infrastructure

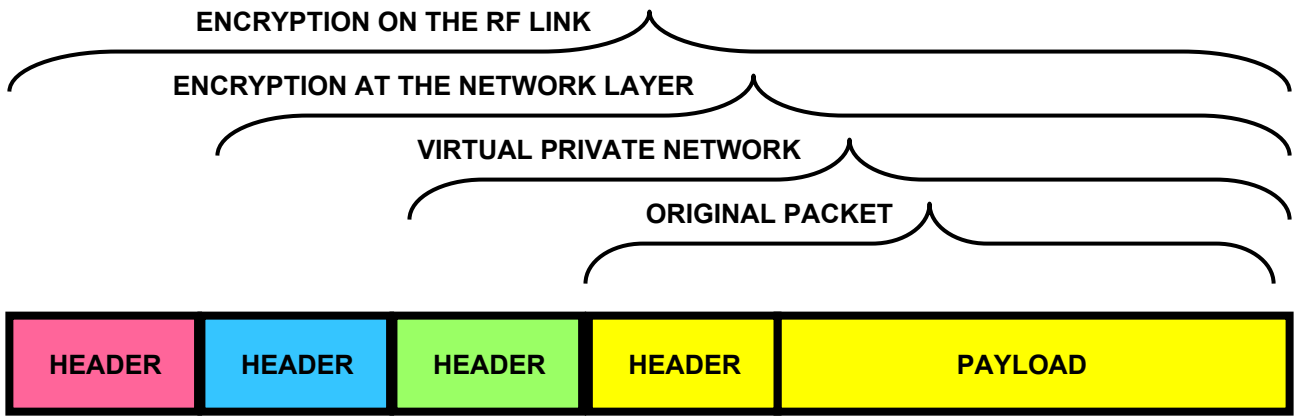


Encrypting wireless links makes it very difficult to share infrastructure. This is a policy issue.

ACME SHIPPING

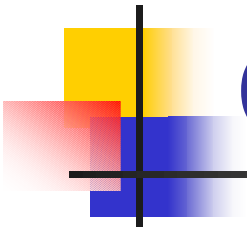
Security

- Security ↑ Bandwidth Utilization ↓
- Security ↑ Performance ↓
- Tunnels Tunnels Tunnels and more Tunnels
- Performance ↓ Security ↓
  ⇒ User turns OFF Security to make system usable!
- Thus, we need more bandwidth to ensure security.



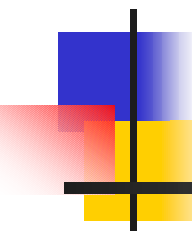
Additional and Future Security Solutions

- AAA
  - Routers (available today)
  - Wireless bridges and access points (available 2002)
- IPSec on router interface
- Encrypted radio links
  - IPSec, type1 or type2, and future improved WEP



Conclusions

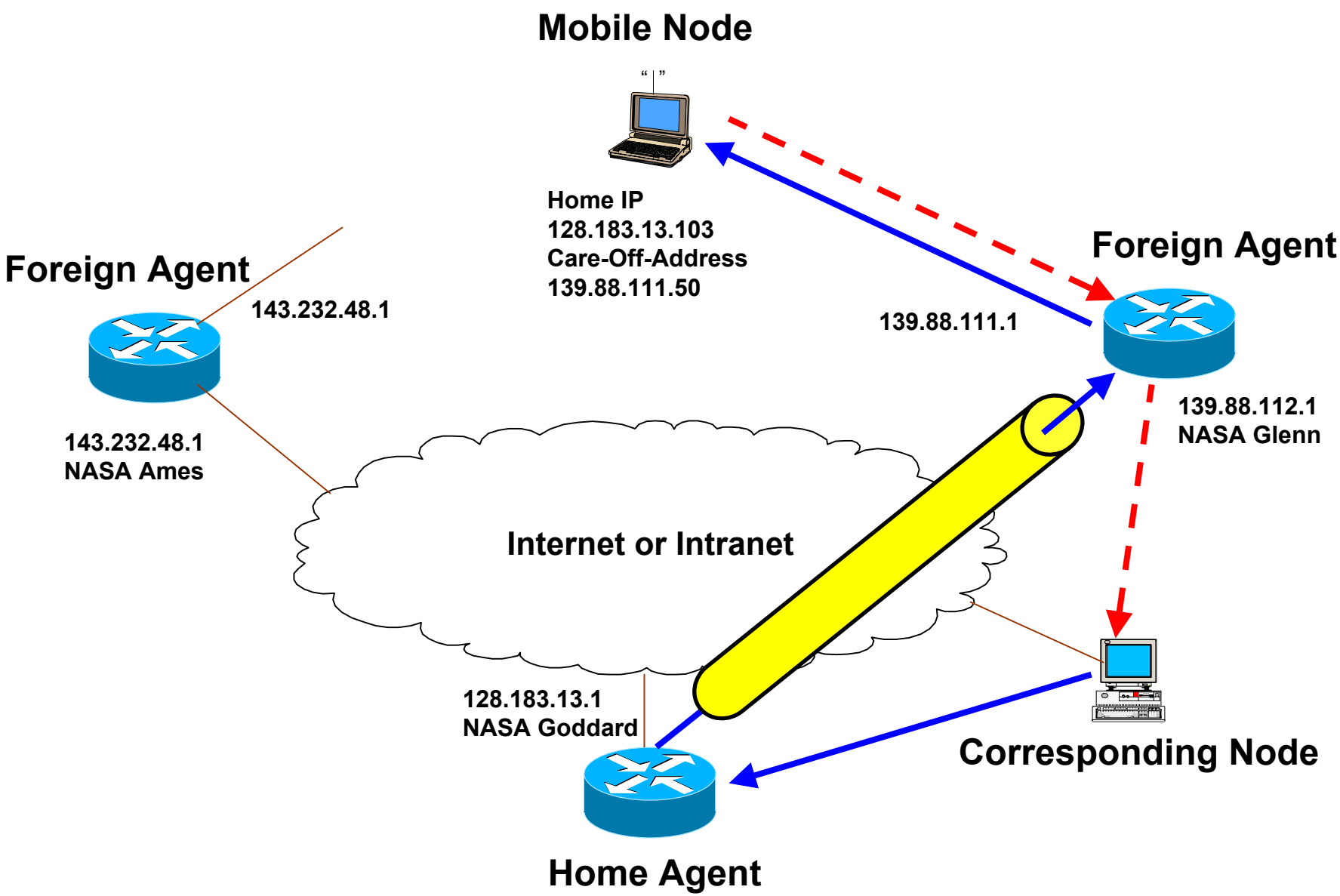
- Security Breaks Everything ☹
  - At least it sometimes feels like that.
- Need to change policy where appropriate.
- Need to develop good architectures that consider how the wireless systems and protocols operate.
- Possible solutions that should be investigated:
  - Dynamic, Protocol aware firewalls and proxies.
    - Possibly incorporated with Authentication and Authorization.



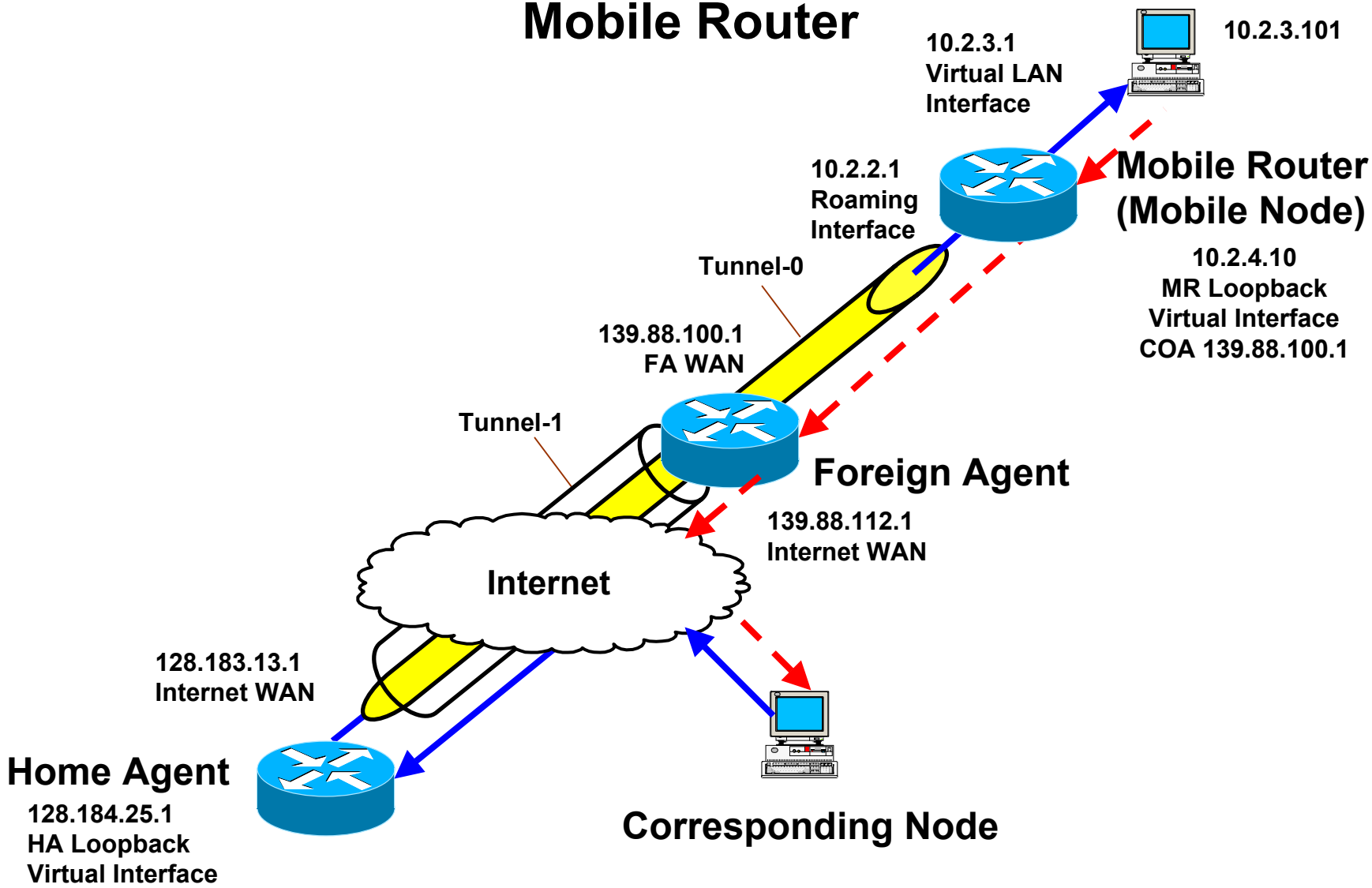
Moblile-IP Operation

IPv4

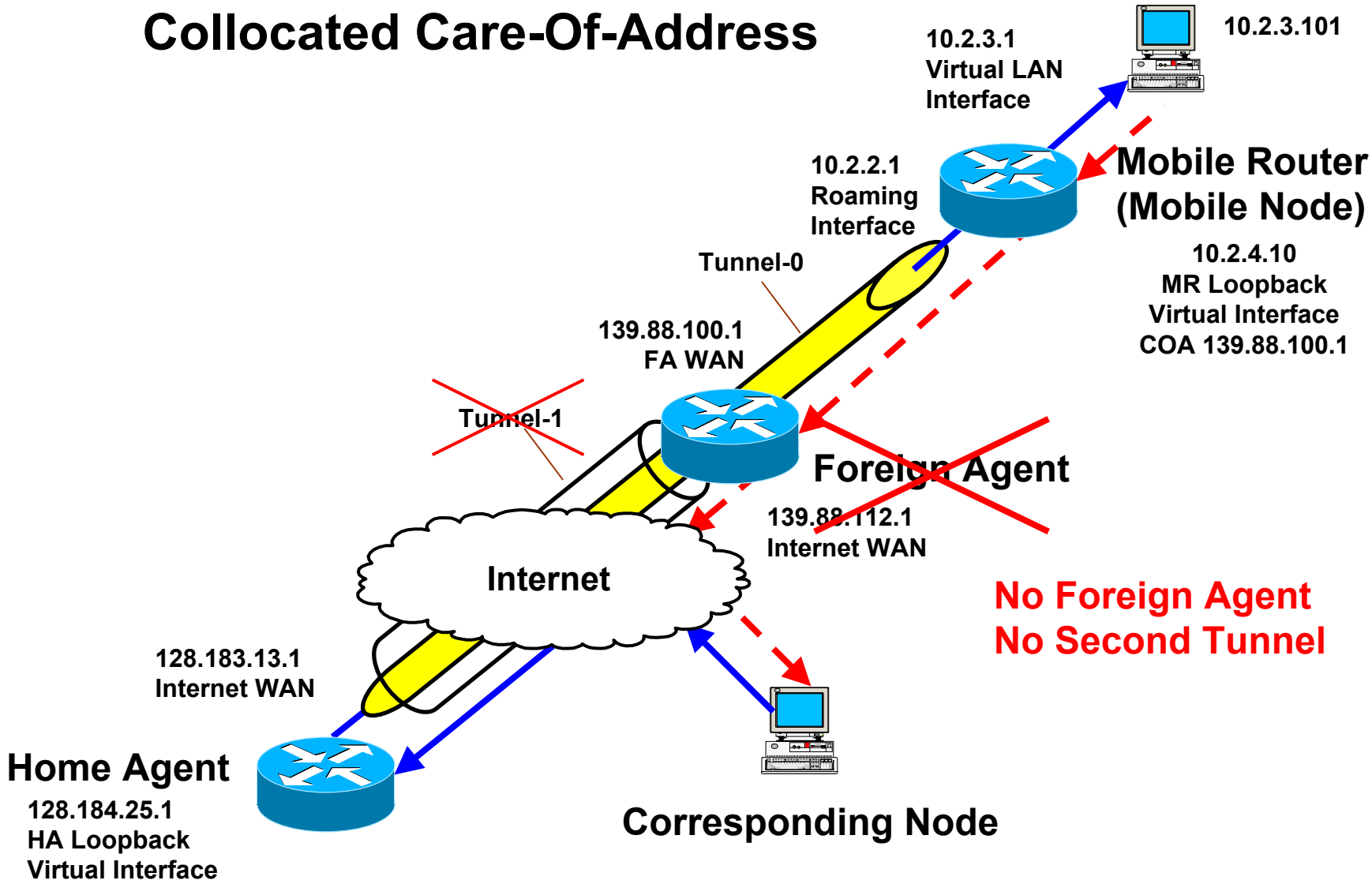
Mobile-IP (IPv4)



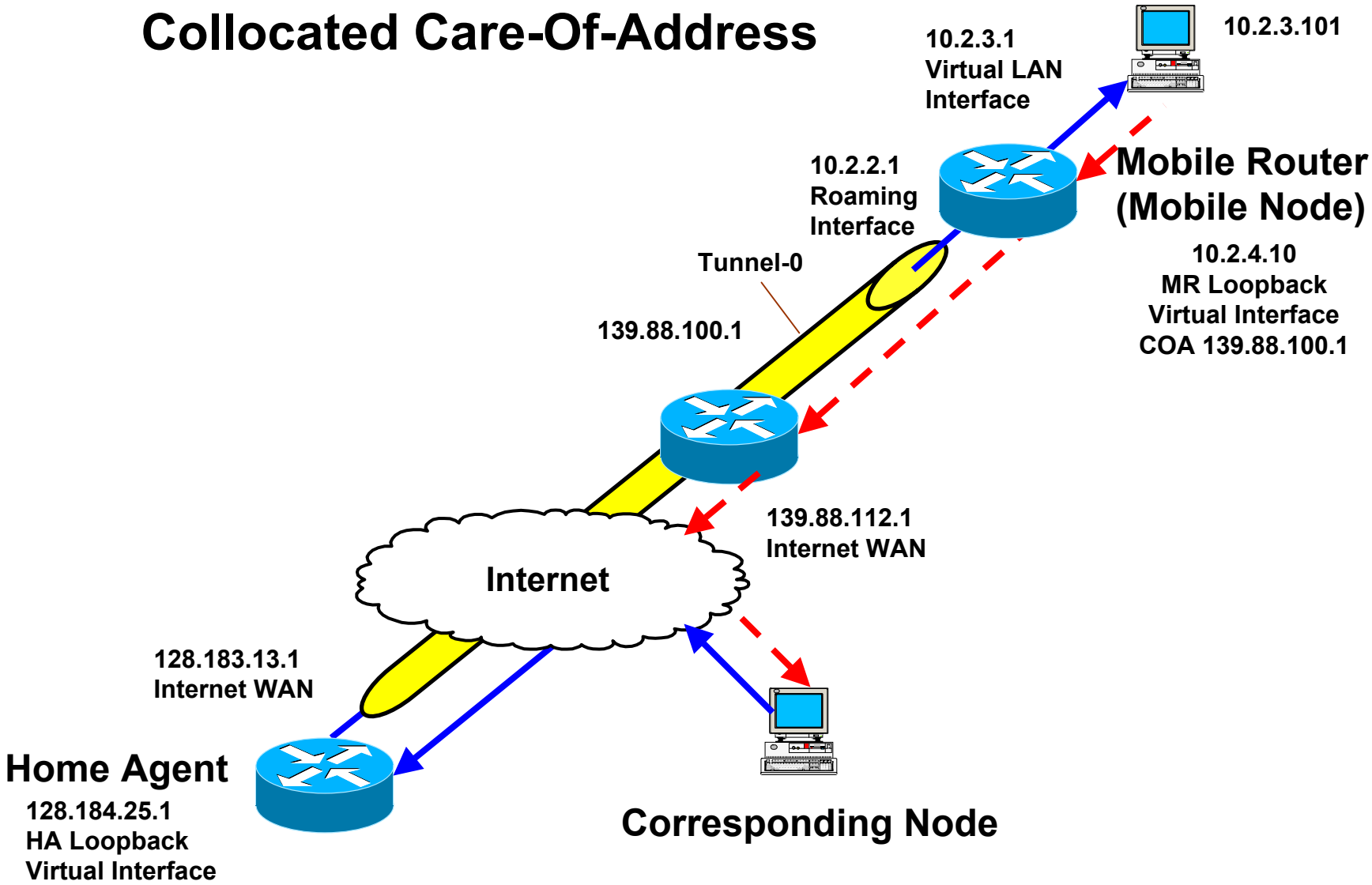
Mobile-Router (IPv4)
Mobile Router

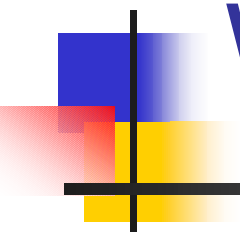


Mobile-Router (IPv4)
Collocated Care-Of-Address



Mobile-Router (IPv4)
Collocated Care-Of-Address



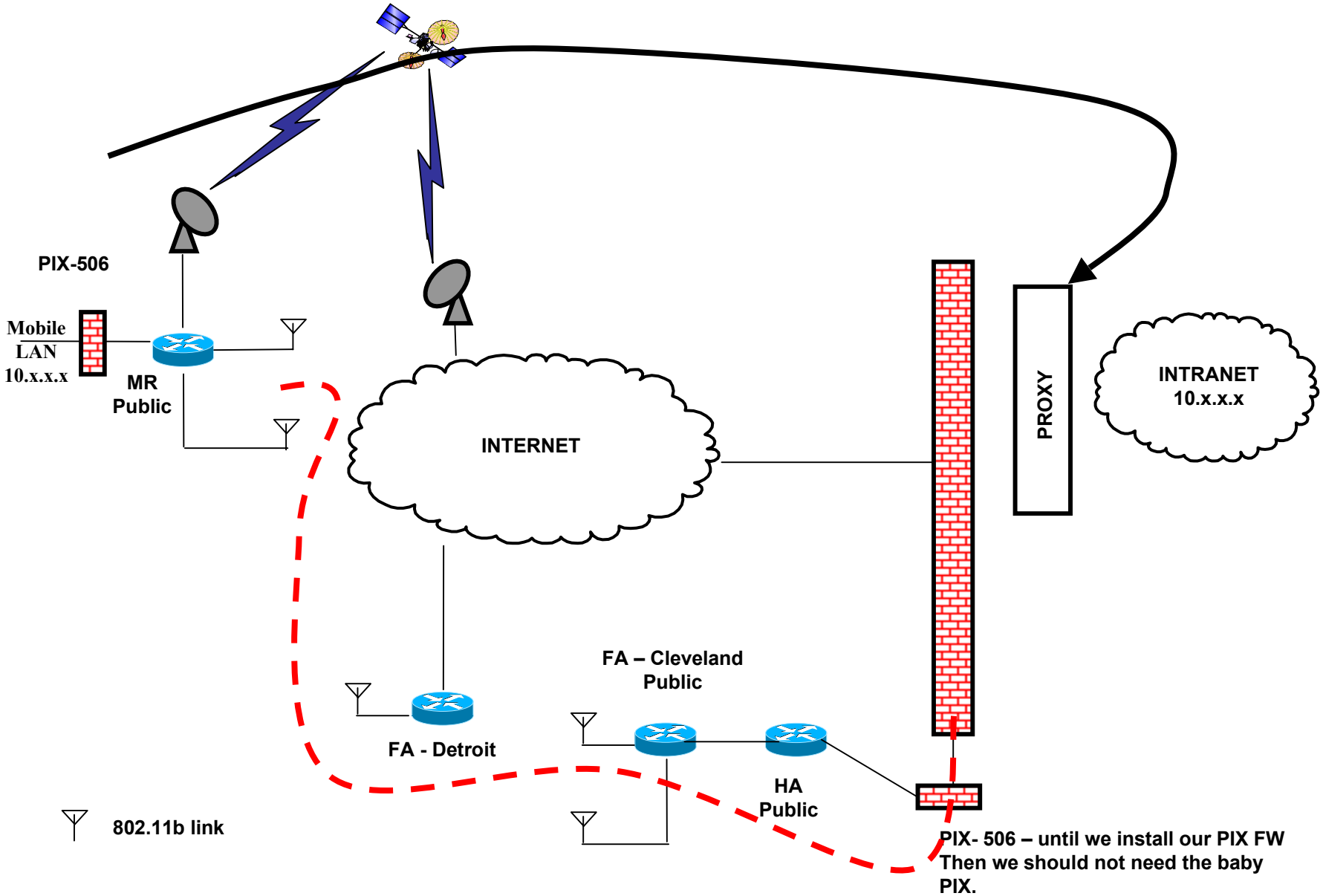


What's Next

The End Game

Mobile Networks

- Share Network Infrastructure
  - USCG, Canadian Coast Guard, Commercial Shipping, Pleasure Boaters
  - Open Radio Access / Restricted Network Access
    - Authentication, Authorization and Accounting
- Architecture
  - Limited, experimental deployment onboard Neah Bay
    - Move RIPv2 routing from Fed. Bldg to Neah Bay
  - Move to full scale deployment
    - Requires full commitment

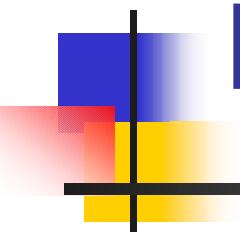

PIX-506
Mobile
LAN
10.x.x.x
MR
Public
INTERNET
PROXY
INTRANET
10.x.x.x
FA – Cleveland
Public
FA - Detroit
HA
Public
802.11b link
PIX- 506 – until we install our PIX FW
Then we should not need the baby
PIX.

HA Outside Main Firewall

- Firewall between MR interfaces and public Internet as well as the HA and Private Intranet.
- Reverse tunneling required as requests from MR LAN hosts must pass through Proxy inside main firewall.

Areas that need to be addressed

- Home Agent Placement
  - Inside or Outside the Firewall
- AAA Issues
  - Open Radio Access / Restricted Network Access
  - Secure Key Management
- IPv6 Mobile Networking Development
  - Work with industry and IETF
- Develop radio link technology
  - Enable better connectivity throughout the world for both military and aeronautical communications (voice, video and data).



NASA's Needs

Mobile Networks

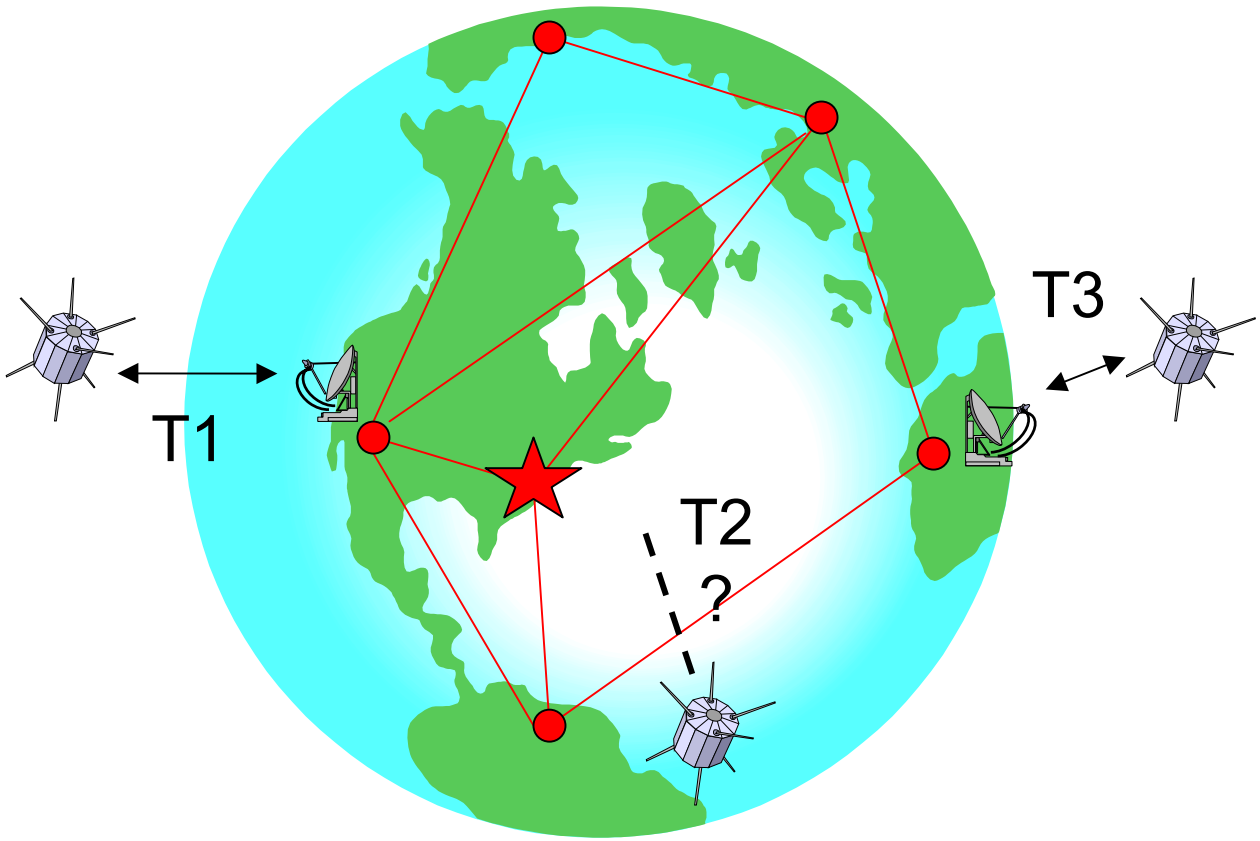
Relevant NASA Aeronautics Programs

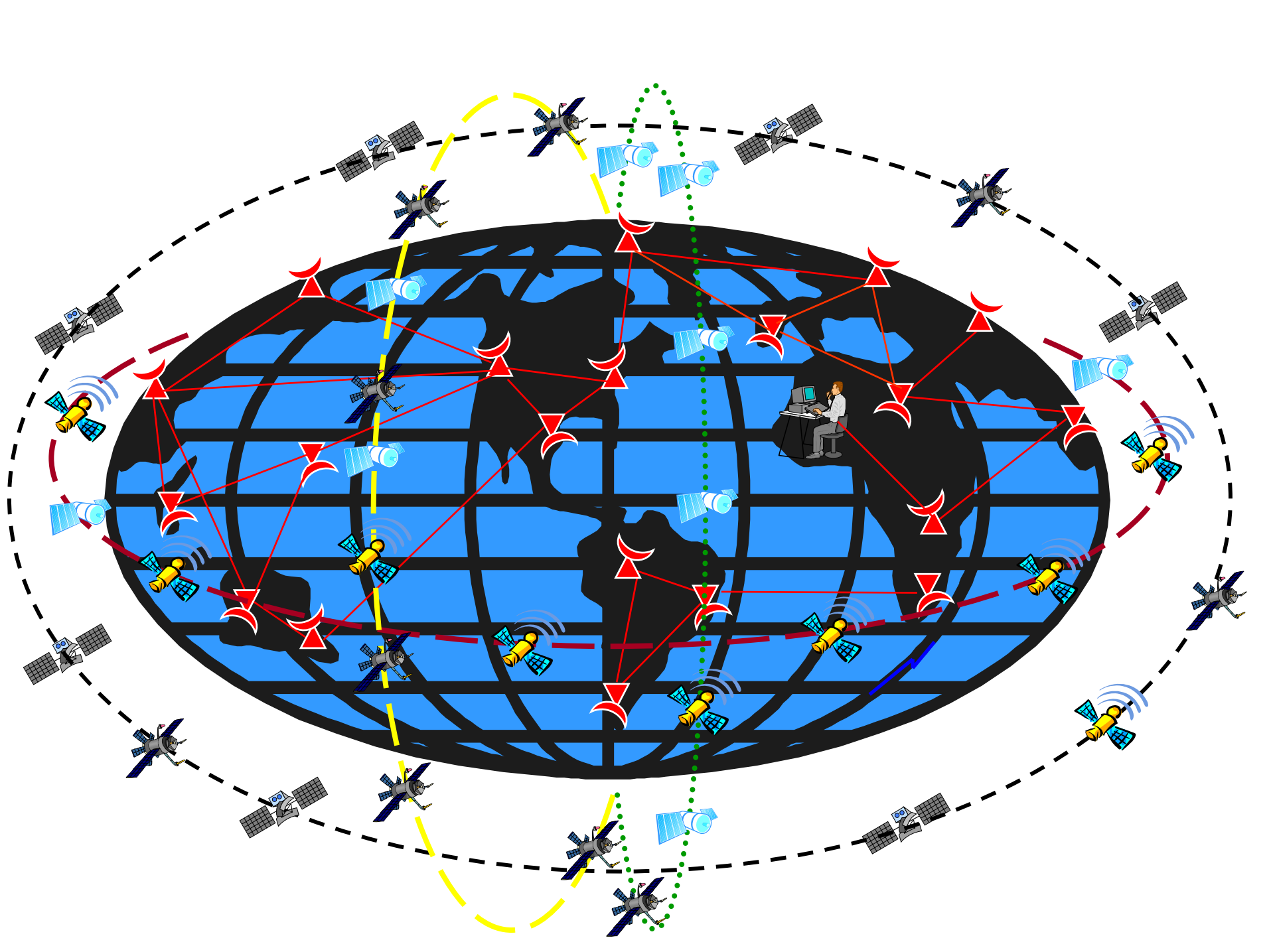
- Advanced Air Transportation Technology (AATT)
- Weather Information Communication (WINCOMM)
- Small Aircraft Transportation System (SATS)

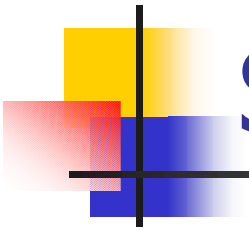
Aeronautic Networking Issues

- Move to IPv6
  - IPv6 Mobile Networking
- Authentication, Authorization and Accounting
- Bandwidth, Bandwidth, Bandwidth
- Media Access
- Policy
  - Sending of Operations over Entertainment Channels

Earth Observation





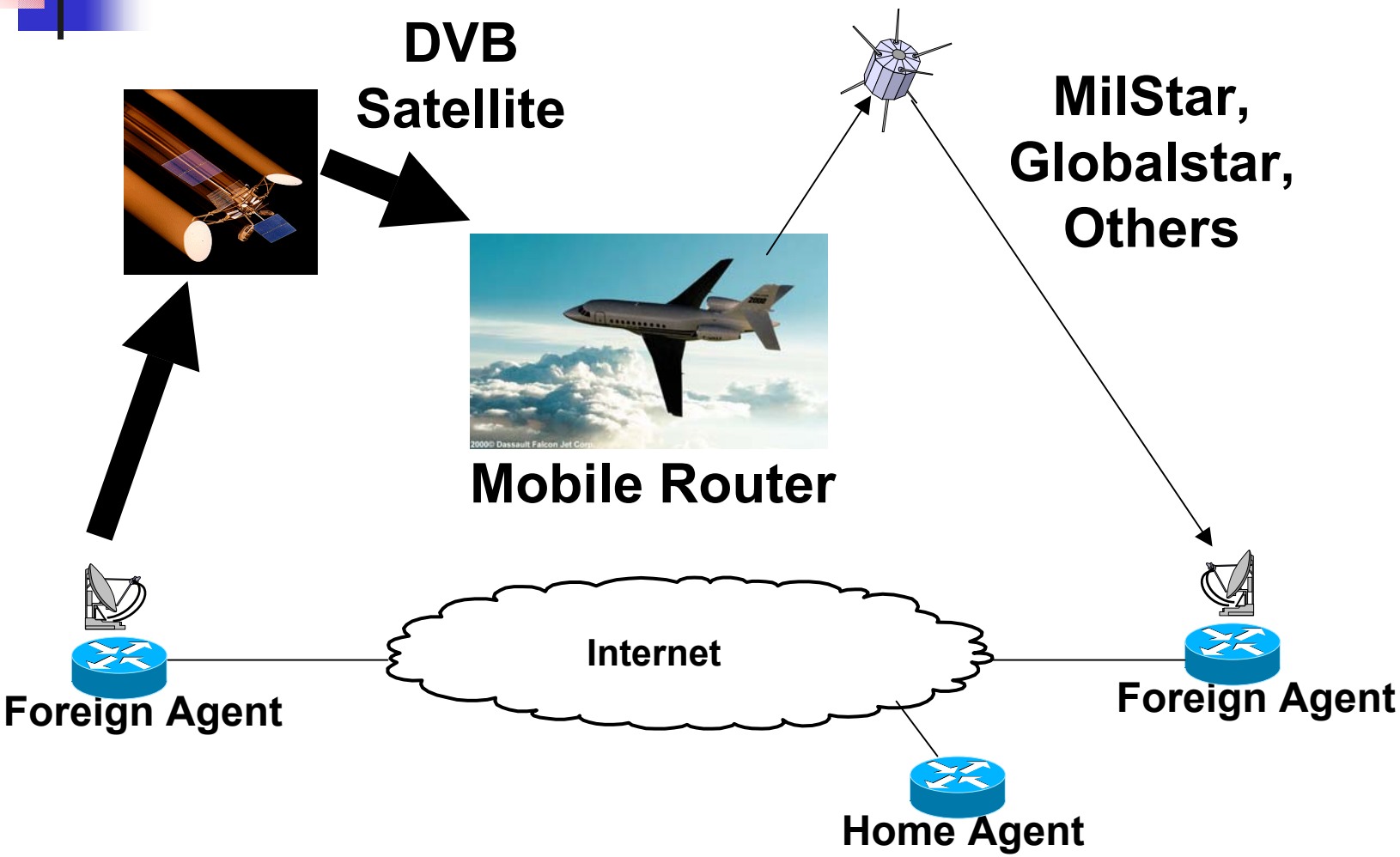


Space Flight Implementation

- Sharing Infrastructure
  - Common Media Access
  - Common Ground Terminal Capabilites
  - Common Network Access
    - AAA
  - Common Modulation and Coding
    - Software Radio

Backup

Asymmetrical Pathing



Neah Bay

Papers and Presentations

http://roland.grc.nasa.gov/~ivancic/papers_presentations/papers.html

or

http://roland.grc.nasa.gov/~ivancic/

and pick

"Papers and Presentations"